Exhibit 7

Arthur Kenzie: A Blackhole in the Security Industry

Mon Jan 23 00:17:22 CST 2012

Jericho

Introducing Arthur 'Wesley' Kenzie, aka Securikai

Late in December of 2011, HD Moore received a curious email from "Arthur (Wesley) Kenzie" notifying him that Kenzie had "important information to discuss with you regarding an email vulnerability that I have discovered affecting your organization." The mail was sent to HD at his personal domain "digitaloffense.net", where he is the only person receiving mail. Kenzie goes on to say that more information about the vulnerability can be found on his web site under the category "Black Hole" email vulnerability.

In short, Kenzie's "black hole email vulnerability" is simply the act of creating a domain that is very similar to a target domain, and accepting email sent to any address at that domain. For those of you who have been in the security industry for more than a year, you probably know this practice as Typosquatting. Wikipedia defines this as "*a form of cybersquatting, and possibly brandjacking which relies on mistakes such as typographical errors made by Internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to an alternative website owned by a cybersquatter.*" Rather than a "vulnerability in HD's organization" as Kenzie framed it, this is a well-known occurrence on the Internet that happens to be routinely exploited by unsavory characters.

After HD replied to Kenzie, the real motivation behind the mail came out

quickly. For the low price of $295.00, along with a "negotiated or mediated non-improvident fee in consideration of my expertise in bringing this vulnerability to [his] attention and in ensuring that no malevolent entity is able to exploit it for their own purposes", HD could get the domain Kenzie registered as his own. To encourage HD to accept this incredible deal, Kenzie mentions that he has already intercepted six emails that were meant for HD.

When HD didn't jump at this incredibly generous offer, Kenzie mailed back days later asking if HD would object to him posting something about "[HD's] vulnerability" to his blog. This second form of motivation, essentially "pay me or I will try to embarrass you", also did not work, and HD opted once again not to buy the domain. In a pathetic attempt to justify his actions, Kenzie explained his actions as having a goal to "increase awareness".

Arthur 'Wesley' Kenzie's actions appear to be a textbook case of extortion.

What Is REALLY Old Is New Again

Creating a domain that is similar to an existing one, but changing a letter that is commonly mistyped, is called Typosquatting (one form of Cybersquatting). Such domains are so prevalent that some security companies discover hundreds or thousands at a time. One recent study claims that "80% of mistyped URLs lead to typosquatting sites".

The act of typosquatting goes back over a decade. One of the more notable instances was HTMAIL.com, a common typo for Microsoft's HOTMAIL.com. HTMAIL.com was registered on April 30, 1997, making it almost 14 years old. Microsoft's own site was similarly typosquatted, when someone registered MIRCOSOFT.com in 1999. An article on digg.com covers the 10 Most Audacious Typosquatting Cases Ever.

The World Intellectual Property Organization (WIPO) is an organization that

handles domain name disputes based on copyright or trademarks. As far back as July 15, 2000, WIPO was arbitrating such disputes. In 2005, Google was awarded the rights to several typosquatted domains registered and set up with the intent to infect visitors with malware.

For Kenzie to claim that he "discovered this vulnerability" is absurd. Anyone that has been on the Internet for a few years should be familiar with this practice. Further, as a researcher, Kenzie opted not to do the first thing in the research process; search to determine if the "vulnerability" has been discovered already. The most embarrassing part of all this, is that Kenzie firmly demonstrates he doesn't fully understand the issue, or how the fundamentals of email work. In his first blog post on the "blackhole email vulnerability" he claims:

> Prior to my registering the mis-spelled domain names, those emails would effectively be garbage that just disappeared without any indication to the sender or recipient.

Anyone who has sent a mail to a non-working or non-existent email address has seen this statement is wrong. Email servers have had functionality that returns the message to the sender in the case it couldn't be delivered for decades. Unless the sender filtered such bounce messages, they would be aware that the mail was not delivered. Perhaps Kenzie is just that new to email and the Internet, and has not run into this before, which does beg the question of his qualifications to provide any technical services.

May Have Fractured an Occasional Law or Two

Kenzie's practice of registering domains with similar names to existing company domains, intercepting email intended for the company, and offering to sell the domain back to the company after hyping this "vulnerability" appears to violate several Canadian laws (where he currently lives). The following represents my opinion and interpretation of the law as a layman, as I am not a lawyer.

Intent

One aspect of many criminal charges is the matter of intent. For example, intentionally striking and killing someone with your car results in a much more severe penalty (e.g., murder) than if it is an accident or due to negligence (e.g., vehicular homicide). In this case, Kenzie makes his intent very clear. From the emails sent to HD and other companies, a few of Kenzie's comments are noteworthy:

> "... it would be irresponsible of me not to give serious consideration to any reasonable offer you might be prepared to make for it."
>
> [..]

> "Alternatively, I would immediately agree to transfer the domain to your organization for a one-time nominal price of $295 provided that you would also agree in principle to paying me a negotiated or mediated non-improvident fee in consideration of my expertise in bringing this vulnerability to your attention and in ensuring that no malevolent entity is able to exploit it for their own purposes."
>
> [..]
>
> "Also, would you object to my posting something on my blog about your vulnerability? Or would you like to have the opportunity to comment before I publish something about your vulnerability?"

Kenzie is registering a domain, intercepting mail, and using that as leverage to motivate a person or company to pay 35 times the price he paid for the domain. When the company doesn't show interest in purchasing the domain, Kenzie goes on to say that he will write a blog about it which threatens negative publicity.

Further, consider that what Kenzie calls "research" is closer to an unethical business model. He did not set up a few domains in order to write a paper detailing the vulnerability. According to DomainTools, Kenzie has registered 311 domains historically and actively maintains 134 of them at the time of this article [Update: List of domains registered to 'Wesley Kenzie' as of 2-2-12]. Kenzie registers his domains through GoDaddy, which offers a discount for bulk domain registration. Currently, registering 134 domains would cost $8.29 each, meaning Kenzie has spent at least $1,102.57 registering his current active domains, and another $2,578.19 for previous domains. Based on his asking price of $295, he would have made $39,235 for active domains (not counting securikai.com) and $91,745 for historical domains totalling $131,275; and that doesn't account for his "negotiated or mediated non-improvident fee".

This makes it clear that Kenzie's intent is not research as he claims, but profit.

Extortion

When a person unlawfully obtains money from a person or institution through coercion, they are committing extortion. Coercion is defined as "forcing another party to behave in an involuntary manner by use of threats or intimidation or some other form of pressure or force." When Kenzie sends an email asking for an unreasonable amount of money for a similar domain name, saying that he intercepted private correspondence intended for the person, and threatens to write a negative blog if they don't pay, he is guilty of extortion.

As a resident of Canada, Kenzie's actions are illegal under Criminal Code (R.S.C., 1985) section C-46, subsection 346:

> 346. (1) Every one commits extortion who, without reasonable

justification or excuse and

with intent to obtain anything, by threats, accusations, menaces or violence induces or

attempts to induce any person, whether or not he is the person threatened, accused or menaced

or to whom violence is shown, to do anything or cause anything to be done.

Cybersquatting

The act of cybersquatting is illegal in the United States under the Anticybersquatting Consumer Protection Act (ACPA). Kenzie lives in Vancouver, British Columbia, outside of the U.S., and seemingly out of the jurisdiction of this law. In reality, Kenzie faces two different aspects of the law, both applicable to him in Canada.

According to Zvulony & CO, a law firm based in Toronto, Canada, if a company approached by Kenzie were to sue, they would have to prove that the Kenzie registered domain name is "confusingly similar" to their trade-mark. For some of the companies he has tried to extort, this would be easy to do in theory. Not only is the typosquatted domain confusingly similar, Kenzie demonstrates that he receives mail at the domain intended for the company. Kenzie practically makes the case for the companies he is going after.

In addition to the Canadian courts likely siding with his victims, Kenzie also has to deal with the U.S. ACPA. Zvulony & CO write that "a Canadian registrant can be sued under [the ACPA]". Kenzie's actions fall squarely within the scope of the ACPA, and his actions could have legal repercussions.

Unfair Competition

Under Canadian law, Kenzie would also be responsible for 'unfair competition'. Per the Trade-marks Act (R.S.C., 1985, c. T-13):

7. No person shall

(b) direct public attention to his wares, services or business in such a way as to

cause or be likely to cause confusion in Canada, at the time he commenced so to

direct attention to them, between his wares, services or business and the wares,

services or business of another;

[..]

(e) do any other act or adopt any other business practice contrary to honest industrial

or commercial usage in Canada.

Zvulony & CO go on to write:

> If you do not have a registered trade-mark, you must sue the offending registrant for the common-law tort of passing-off. The allegation in a passing-off case is that the registrant is providing unfair competition by making it seem like his or her business is associated with yours. You would be required to prove that the registrant has caused actual or potential harm to your business by infringing your trade-mark and misleading the public.

Again, since Kenzie is intercepting email intended for the victim company and using it to leverage them into paying an exorbitant price for the typosquatted domain, he is essentially proving the damages for the victim company.

Interception of Communications

Under Canadian law, Kenzie would likely be guilty of 'interception of communication'. Per the Canadian Criminal Code (R.S.C., 1985, c. C-46):

> 184. (1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device,
>
> wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment
>
> for a term not exceeding five years.

Note that the law specifies "wilfully intercepts a private communication", something Kenzie admits to in his emails to the victim company.

The "Data Breach" Angle

Through a reliable source, I have been told that Kenzie has recently started increasing the pressure on companies he targets by invoking the threat of data breach laws and mandatory disclosure. The exact contents of the mails he *sends* has not been confirmed, but they have been described in some detail. Apparently, Kenzie has engaged a law firm or is using the name of one as a

threat and saying that should any sensitive mails reach his typosquatted domains, that the company may be liable under United States breach laws (which vary by state).

Kenzie's argument goes something like this: if a third-party emails sensitive information that falls under these laws (e.g., names, addresses, Social Security Numbers), and that information ends up in Kenzie's email due to him registering the domain and blackholing all email destined to it, then it constitutes a data breach that the company is liable for. This is certainly an interesting argument, and one that has not been tested in any court I imagine. There are two aspects to this that Kenzie has apparently failed to consider though.

First, the sender of the email would be liable for the disclosed data, not the recipient. If Kenzie is typosquatting "BigCompany", and "Contractor" sends the sensitive information to Kenzie, then the contractor is liable. While notification of such a breach may be sent out from BigCompany, their culpability in the disclosure is simply not there. It would behoove them to investigate, notify, and consider switching to a contractor that was more prudent in the handling of data.

Second, and more importantly, Kenzie has not considered his own liability in the disclosure. If he had not registered the domain and configured it to accept mail destined to any address, the disclosure would not have happened. "Contractor" would have emailed the sensitive information, and their own mail server would have been unable to resolve the misspelled domain. This would in turn cause their own mail server to return the mail to the sender saying "unknown domain" essentially. The sensitive information would not have left their computers to begin with. All of this ties back into Kenzie's actions breaking laws regarding wilfully intercepting private communication, cybersquatting, and unfair competition.

In Conclusion, A Few Simple Truths

Regardless of the legal implications and my interpretation of the law, there are a few simple truths regarding Arthur 'Wesley' Kenzie. The first, and most important, is that Kenzie's actions are unethical. Registering hundreds of domains and intercepting email in an attempt to motivate companies to pay him outrageous fees is not the action of an ethical security consultant.

In addition, Kenzie's technical prowess is certainly questionable. Not only did he neglect to research the "blackhole email vulnerability", he has demonstrated that he doesn't fully understand the basics of the Simple Mail Transfer Protocol (SMTP) and the clients/servers that implement it. Failing to understand the basic concepts make it difficult to believe he has any mastery of the more advanced concepts that make up network security.

Perhaps the most surprising aspect to Kenzie's actions, is that he is a contributor and advocate of TOR, self-described as "free software and an open network that

helps you defend against a form of network surveillance that threatens personal freedom and privacy". Resorting to extortion to make money while claiming his actions are done to "raise awareness of security issues" is an insult to the individuals who actually raise security awareness through legitimate security research.

If your company has received email from Kenzie regarding this "vulnerability" or an offer to buy one of his domains, I encourage you to publish the mails and help expose his unethical business practices. As always, you can also mail Kenzie at wkenzie@securikai.co and give him a piece of your mind.